“养龙虾”,金融圈谨慎入场

“你养虾了吗?”近日,全网都在为OpenClaw“龙虾”疯狂,从个人端的效率提升,到企业端的流程自动化,这一开源AI智能体几乎席卷所有科技应用甚至社交场景,不过在金融圈却不尽然。

3月10日,就全民“养虾热”及是否有意布局OpenClaw,记者向多家银行、消金公司、支付机构进行了采访,大多表态“太火了,需要先沉淀观察”,也有人士直言,OpenClaw不适配金融,尤其要注意其中的数据安全风险。业内人士认为,这场“养虾热”中,互联网银行、消金公司没有跟风部署,支付机构技术团队按兵不动,背后是对资金、数据和信息安全的重要考量。

集体冷静

“养虾”热,在金融圈却集体“哑了火”。“因为金融行业严格要求保密性,这一AI应用有可能存在数据和信息安全的风险隐患。”一消金公司从业者直言了他的顾虑。

“有一定价值,但在消金核心业务领域始终面临多重风险。比如合规方面,开源智能体很难满足监管对于风控等核心业务的要求;再如安全方面,开源智能体可能导致信息泄露风险等。”另一消金公司从业者同样提及。

总结来看,核心原因还是金融行业强监管、高风险的底线要求。

对消费金融公司来说,若通过AI智能体自主完成客户授信、风控审批到信贷发放等流程,效率确实能翻倍,但一旦出现过度放贷、授信失误或信息泄露,责任该怎么算?风险谁来承担?这也正是最大的风险,即技术自主性与金融行业合规安全要求的天然冲突。

“这是雷区。”不少消金从业者表态,没人愿意为了技术尝鲜,触碰数据和安全高压线,“感觉OpenClaw有点太火,对其价值还是要再沉淀观察一下。”也有人称,短时间内,金融行业更多还是偏审慎,但不排除分层渗透的可能性。

支付机构的焦虑则更直接,每一笔交易都关乎资金安全,容不得半点“算法黑箱”。易宝支付联合创始人余晨接受记者采访时提到,OpenClaw带动的开源智能体热潮,代表行业从对话AI走向自主执行,方向有价值,但公司仍对开源框架保持开放观察、审慎落地的态度,自主执行、权限开放与合规风控的底线要求存在天然冲突,金融行业必须先把安全与可控做扎实。

在银行方面,有一线员工表示:“目前行里使用OpenClaw的人并不多。在我们看来,OpenClaw相当于一款权限较高的AI软件,能够授权操作电脑,直接执行指令。这类功能我们一线员工不会用,大概率只有技术部门在少量测试使用。”

一位银行业务部门负责人直言,这类开源产品在使用过程中需要用移动设备远程控制终端个人电脑,即便宣称信息隔离,但银行依然高度谨慎,基本不会直接使用。

适配度较低

从金融行业视角来看,余晨认为,开源智能体最大的价值在于能实现流程自动化、提升效率,把人从重复劳动中解放出来,为业务降本增效,但也有着对应的风险,是智能体自主决策带来的不可解释、不可控问题,以及数据安全、越权操作等隐患,会直接触碰金融领域的合规底线。

“我觉得个人玩玩、办办公还行,要应用在业务上‘坑’太多,比如数据安全风险、资金安全问题等。”另一支付公司从业者则说道。在他看来,支付业务的风控环节已经较为完善,盲目尝试这类AI智能体反而暗藏风险,“万一适配出问题,可能引发交易中断、资金清算错误,后果不堪设想。”

“银行做科技建设,第一优先级永远都是安全合规。”一家地方农商行科技部门人士介绍,当前,银行对开源项目布局的核心顾虑集中在两大方面:一是数据安全风险,开源代码公开导致漏洞较多、“后门”难以排查,数据容易出现泄露隐患;二是操作管控风险,哪怕产品厂商宣称能够实现信息隔离,只要涉及跨设备、跨网络控制,就存在被劫持、截屏、录屏、越权操作的可能,这些行为都直接触碰金融安全“红线”,银行绝对不会冒险使用。

业内人士认为,金融业作为强监管、高风险行业,对此保持高度克制是理性且必要的。联储证券研究院副院长沈夏宜解释,金融行业的特殊性在于,其核心业务涉及资金安全、客户隐私和系统性风险,任何技术创新都必须以风险可控为前提,不能像互联网行业那样采取“快速迭代、试错跑通”的模式。

在沈夏宜看来,现阶段,OpenClaw与金融行业的适配度仍处于较低水平。一方面,其核心的端到端自动执行能力与金融行业的合规要求存在天然矛盾,权责边界模糊、算法可解释性不足等问题,难以满足银行、消金、支付等机构的监管红线。另一方面,金融行业对数据安全、业务稳定性的要求极高,而OpenClaw部分实例存在安全漏洞、第三方技能市场风险等问题,叠加金融业务的复杂性,目前仅能在金融机构的非核心场景进行小范围试点,无法进入授信、风控、资金清算等核心领域,整体适配仍需长期优化。

并非排斥

值得注意的是,金融行业的“冷静”并非拒绝AI,而是拒绝盲目跟风。在银行业从业者看来,OpenClaw这一波开源AI智能体浪潮,本质上是一次AI应用范式变革的全民普及。大模型的能力已经突破了临界点,市场需要这样一波浪潮让用户深刻意识到:AI已经不再仅仅是辅助工具,不再是只会提供建议的“咨询师”,而是真正能落地做事的“实习生”。

该银行业从业者称,像OpenClaw这样的AI应用范式是未来技术发展的必然趋势。因此,对于金融行业而言,这并不是“不敢用”或“现阶段不适合用”的问题,而是如何小心谨慎、循序渐进地将其用起来的问题。金融机构的克制,更多是出于对合规与风险的敬畏,而非对技术的排斥。

从短期来看,开源智能体最大的价值在于显著提升金融服务的效率,降低运营成本,从而使金融服务更加普惠。从长期来看,这种具备主动执行任务能力的智能体,或许能为行业带来全新的业务模式,创造增量价值和新的市场机会。

然而,风险同样不容忽视。前述银行业从业者补充,在合规、安全和投入层面,金融机构确实存在顾虑,最大的风险可能集中在应用层面。智能化的普及使得很多事情的执行门槛大幅降低,这既包括创造价值的好事,也包括潜在的恶意行为。因此必须切实增强风险防范意识,提前做好应对准备。

事实上,在AI技术的应用上,已有多家机构悄悄开启“定制化探索”,在智能化布局上实现新的突破。

银行层面,前述银行业从业者介绍,目前,该行重点在风险贷后管理、客户服务、电话营销等场景进行了深入投入与落地。同时,在授信审批、日常运营、合规安全等核心环节,也有广泛的AI应用探索。“如果开源AI智能体要真正进入金融核心场景,需要优先解决技术层面的安全合规问题。”在他看来,在现阶段及未来的一段时间内,权责认定的前期工作仍需以“人”为主导,必须确保在关键业务环节有专业人员进行严格管控。

招联消费金融介绍,目前,招联已经形成了包括消保、合规、资管、运营、风险、决策、研发、中医八大核心智能体以及若干办公智能体,深度赋能各业务板块提质增效。

支付机构方面,连连数字相关负责人也提到,近年来,连连数字全面推进AI技术在风控、运营及客户服务的全链条融合,以及接入主流AI大模型,其中,连连数字自主研发的专有技术平台,可为客户提供涵盖支付、资金转账、全球资金分发、智能汇兑处理以及智能风险管理等在内的一站式综合服务。

渐进融合

热潮过后,业内人士认为,金融行业并不会迎来“OpenClaw落地潮”,而是进入一个审慎探索、渐进融合的新阶段。“金融行业其实是最早应用AI的垂直领域,因为金融科技行业天生就有大量的交易数据。”余晨介绍,金融业应用的人工智能技术主要分为两类:一类是底线应用,用人工智能技术作为护栏为业务保驾护航,比如反洗钱等领域都会大量应用人工智能技术;另一类是顶线应用,能够给企业带来更多的生意和业务。

在余晨看来,未来金融AI的应用空间非常广泛,企业可以借助AI优化智能客服、提升用户体验,利用大模型开展交叉营销、挖掘新的销售线索,同时在风控、合规自动化等方向持续深耕,让AI技术真正服务于业务与用户价值。

“目前银行、消金、支付等机构的智能化转型,都是走辅助式路线,没有盲目追求全流程自动化,布局比较务实,这既契合金融强监管的属性,也贴合技术现状和商业环境。”博通咨询首席分析师王蓬博评价,在他看来,后续开源AI智能体若要进入金融核心场景,必须先解决算法可解释、可追溯,不能有黑箱,要满足金融强监管、高安全的要求;另外要明确权责边界,界定好各方责任,契合金融行业的严肃性,此外要保证数据合规,保障用户敏感信息不泄露,兼顾商业诉求,找到开源与机构核心利益的平衡点,且保留人工干预权限,避免不可逆的风险。

小场景落地

结合行业发展趋势与监管要求,对于未来5至10年开源工具在银行领域的应用前景,多位银行人士坦言,只有在个人信息保护做到绝对严密、技术实现完全可控,且风险可防可控的前提下,银行才可能对开源工具进行有限度的探索。从可探索的方向来看,主要集中在非隐私类营销推送,即不涉及客户敏感信息的营销场景,以及其他不涉及资金交易、不触碰客户核心数据的辅助环节,避免核心业务与敏感信息面临安全风险。

“这种审慎并非保守,而是对金融风险特殊性的理性回应。金融机构可在试点中积累经验,在可控场景中验证价值,逐步扩大应用范围。”联储证券研究院研究员杜彤彤说道,金融机构应坚持审慎创新的原则,优先在非核心场景试点开源智能体,积累应用经验,逐步探索核心场景的适配方案。

“金融行业还将继续保持审慎态度,不会出现大规模的开源智能体落地潮。”王蓬博同样称,谈及未来金融AI的方向,他认为将聚焦在合规可控、辅助决策、小场景落地这三个核心,重点瞄准风控优化、合规自动化、运营增效等领域,不会盲目追求全流程自动化,会优先选择客服、广告类写作这类低风险、非核心环节落地,避开核心业务的安全和合规隐患。

前述银行业从业者也提到,短期内,金融机构不会盲目追求完全的端到端自动化,而是会更加强化“人在回路”的混合模式,确保人类专家的最终决策权。

其次,注重多智能体协同与人工监督相结合。未来的技术趋势不会是单一智能体的完全自主运行,而是构建“多智能体+人工监督”的复合架构,以应对复杂的金融场景。

此外,要建立完善的AI治理体系。金融机构将普遍建立起包括AI资产清单盘点、风险重要性评估、全生命周期闭环管控等在内的系统化治理机制,确保AI技术的应用始终在安全、合规的轨道上运行。

也有银行人士提到,银行探索开源工具还需满足明确的条件与前提,在行业规范层面,需出台金融行业专属的开源工具应用规范,清晰界定开源工具的应用范围、安全标准与责任归属,为银行应用提供明确的合规指引;在技术层面,开源生态需形成金融级的成熟解决方案,具备漏洞实时监测、快速修复的能力,同时要支持国产化适配与核心技术自主可控,确保开源工具的应用不会影响银行系统的稳定性与安全性。

据《北京商报》 作者:刘四红 宋亦桐

“养龙虾”的第一批受害者出现了?

近期,一股“养龙虾”的风潮席卷社交网络。这并非水产养殖,而是一款名为OpenClaw的AI智能体工具。因其红色龙虾图标,用户配置、调试它的过程,被生动地喻为“饲养”一位数字助手。它宣称能成为24小时在线的“数字同事”,自动处理电脑任务,一时间引发全网追捧,甚至催生出“上门安装月入26万元”的传闻。

然而,热闹还没过去,第一批“踩坑”的人已经出现了:有人稀里糊涂就开始欠费了,有人则在尝试自动操作时,遭遇了文件被全部误删的尴尬,工信部、国家互联网应急中心都发出了相关安全预警。

不少网友称打算卸载OpenClaw,网上也出现不少OpenClaw卸载教程。

据了解,3月10日,某交易平台上已出现卸载OpenClaw的服务。一名IP地址显示在上海的商家报价,上门卸载OpenClaw收费299元(仅限在上海),远程卸载OpenClaw收费199元,并称“安全彻底,无残留”。

“第一批养虾人已经开始卸载了”

3月11日,相关话题“第一批养虾人已经开始卸载了”,引发网友热议。有网友反馈,“养龙虾”过程中,出现了乱删邮件、隐私泄露等问题。

据媒体报道,有网友在网络上分享自己使用OpenClaw的经历,他将自己的工作邮箱交给了OpenClaw打理,指令是:“检查收件箱,提出你想归档或删除的邮件。”他特意附加了“未经许可不要有任何操作”的限制。然而,“龙虾”无视该网友连续发出的“停下来”的指令,疯狂地删除了数百封邮件。

据报道,深圳一名程序员在安装OpenClaw的第三天,因应用程序编程接口(API)密钥被盗,在凌晨收到了高达1.2万元的Token(词元)账单。由于OpenClaw具有极高的自动化权限,一旦密钥泄露,AI便可能在后台疯狂调用模型,让用户在不知不觉中背负巨额消费。

“养龙虾”带来的隐私与安全风险,正持续引发网友担忧。OpenClaw爆火后,也带火了二手交易平台的“龙虾上门安装服务”。然而,近日,上门卸载又迅速成为新的热门业务。

有关部门提示安全风险

此前,工业和信息化部网络安全威胁和漏洞信息共享平台监测发现,OpenClaw开源AI智能体部分实例在默认或不当配置情况下存在较高安全风险,极易引发网络攻击、信息泄露等安全问题。

3月10日,国家互联网应急中心发布关于OpenClaw安全应用的风险提示称,为实现“自主执行任务”的能力,该应用被授予了较高的系统权限,包括访问本地文件系统、读取环境变量、调用外部服务API以及安装扩展功能等。然而,由于其默认的安全配置极为脆弱,攻击者一旦发现突破口,便能轻易获取系统的完全控制权。同时建议相关单位和个人用户在部署和应用OpenClaw时,采取强化网络控制、加强凭证管理、严格管理插件来源、持续关注补丁和安全更新等安全措施。

中国信息通信研究院专家指出,“龙虾”出现以后,受到我国产业界和广大用户的广泛关注,大家积极开展实践应用,推动了我国AI智能体生态的繁荣,但也要注意到,“龙虾”强大的执行能力也给用户带来了严峻的安全挑战。

专家呼吁,党政机关、企事业单位和个人用户要审慎使用“龙虾”等智能体。在发现“龙虾”等智能体的安全漏洞,或者针对“龙虾”等智能体的安全威胁和攻击事件时,可以第一时间向工业和信息化部网络安全威胁和漏洞信息共享平台报送,平台将按照《网络产品安全漏洞管理规定》要求,及时组织处置。

央视网发表评论《养“龙虾”狂欢:我们怕的不是风险,是掉队》,其中提到,普通人该如何与AI相处。或许,不在于更快地养上“龙虾”,而在于自我的认知思考。

其一,追不上技术迭代速度,或成为常态。企图掌握所有AI工具,在指数级进化的技术面前大抵是徒劳的。即便是AI专家,也无法穷尽所有领域。真正的目标,不应是与AI赛跑,而应是让AI为你赛跑,将OpenClaw等工具视为能力杠杆,用你的独特洞察力和创造力去撬动你所擅长的领域和工作。

其二,从“追逐工具”转向“定义问题”。从AI对话中的“提示词工程”,到智能体应用的“工作流编排”,精准提问、整合资源已成为解决复杂问题的关键能力。AI是强大的引擎,而人类应该成为无法替代的“提问者”与“价值判断者”。

其三,用持续学习和行动对抗焦虑。焦虑常源于“想得多,做得少”。多项研究表明,善用AI工具可使办公效率提升20%至80%不等。AI价值不仅在于速度,更在于解放员工,去专注于更高价值的任务。在保障安全的前提下,让AI处理一件复杂任务,节省一小时时间。这种正向反馈和技能习得,对于重建技术自信很重要。

新工具热潮此起彼伏,“龙虾”不是最后一个,今天安装的软件,明天都可能被卸载。但如果能从中沉淀出对问题本质的深刻理解,并驾驭工具,那么这场喧嚣便超越了工具本身。所以,与其再问“我会不会被AI替代”,不如思考“我的不可替代性在何处?”

供稿:《每日经济新闻》 作者:金冥羽 杜波